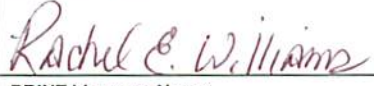
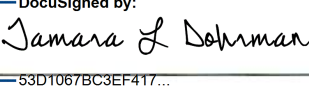
 WASHINGTON STATE DEPARTMENT OF LICENSING		DATA LICENSING CONTRACT FOR DEPARTMENT OF LICENSING'S DRIVER AND PLATE SEARCH (DAPS) SYSTEM		DOL Contract No.: K5572-1	
Contract					
Contract start date Upon execution		Contract end date: August 31, 2018 or when DAPS is transferred to the DRIVES system, whichever is later.		Contract amount Non-financial	
Purpose (brief description) This Data License Agreement establishes the requirements and authorization for the Licensee to receive access to DOL Data through its Driver and Plate Search (DAPS) system.					
Licensee					
Licensee name US Dept. of Homeland Security, Immigration & Customs Enforcement, Homeland Security Investigations			Address 1000 2nd Ave, Ste 2300 Seattle, WA 98104		
Contract manager Rachel Ealy-Williams		(Area code) Telephone 206-442-2286		Email rachel.a.ealy-williams@ice.dhs.gov	
Department of Licensing (DOL)					
Department administration Data Licensing Unit			Division Program and Services Division		
Contract manager Naomi Dickson			Contact address PO Box 2076, Olympia, WA 98507-2076		
(Area code) Telephone (360) 902-3708			Email dapscomm@dol.wa.gov		
Attachments					
This Contract consists of the following attachment(s) and document(s): Data Licensing Statement #1 – Access to DAPS Attachment A, Data Security Requirements Attachment B, Permissible Use Requirements Attachment C, Appropriate Use Declaration (425-008) Employee Access/Change Request form (425-011)					
The terms and conditions of this Contract are an integration and representation of the final, entire and exclusive understanding between the Parties superseding, all previous agreements, writings, and communications, oral or otherwise, regarding the subject matter of this Contract. The intent of the Parties is that the effective date of this Contract shall be upon execution by both Parties. The Parties signing below represent that they have read and understand this Contract, and have the authority to execute this Contract.					
Licensee Signature 		Date 5/31/18		DOL Signature 	
PRINT Licensee Name Rachel Ealy-Williams		Name Tamara Dohrman		Date 6/1/2018	
Print Title Special Agent		Print Title Assistant Director Administrative Services Division			
E-Mail rachel.a.ealy-williams@ice.dhs.gov					

@ice.dhs.gov

REW

This Data Licensing Agreement (hereinafter "Agreement") is between the Washington State Department of Licensing (hereinafter "DOL"), and US Dept. of Homeland Security, Immigration & Customs Enforcement, Homeland Security Investigations (hereinafter "Licensee"). DOL and Licensee may be individually referred to as "Party", or collectively referred to as "Parties."

Pursuant to the mutual terms and conditions herein, and based upon Licensee agreement hereto, the Parties hereby agree as follows:

1. BACKGROUND AND PURPOSE

In accordance with the Revised Code of Washington (RCW), some government agencies may access and receive specific information maintained by the Department of Licensing as part of its vehicle and/or driver records. This information may be accessed through DOL's Driver and Plate Search (DAPS) system, at DOL's discretion.

The purpose of this Agreement is to provide the terms and conditions for authorizing governmental entities to access DOL's DAPS system.

2. LEGAL JUSTIFICATION

The Data shared under this Agreement is permitted pursuant to the following authority: Chapters 39.34 RCW, and Federal Driver Privacy Protection Act (DPPA) 18 U.S.C. §2721 through §2725.

3. DEFINITIONS

As used throughout this Agreement, the following terms have the meanings set forth below:

"Authorized Users" means those individuals authorized by the Licensee to access Data under this Agreement.

"Confidential Information" means information that may be exempt from disclosure to the public or other unauthorized persons under either chapter 42.56 RCW or other state or federal statutes and data defined as more sensitive than "public" and requires security protection. Confidential Information includes, but is not limited to, vehicle legal owner, social security numbers, credit card information, driver license numbers, Personal Information, law enforcement records, agency security data, and banking profiles.

"Data" means information obtained from DOL's DAPS system pursuant to this license and provided to Licensee. This definition inherently includes material that contains Confidential Information.

"Data Security" means defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. This applies regardless of the form the Data may take (electronic, physical, etc.).

"Data Security Breach" means unauthorized acquisition of Confidential Information that compromises the security, confidentiality, or integrity of Confidential Information maintained by the person or business as defined in RCW 19.255.010.

"Permissible Use" means only those uses authorized in this Agreement and as specifically defined.

"Personal Information" means information identifiable to any person, including, but not limited to information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, addresses (except 5-digit zip code), telephone numbers, social security numbers, driver license numbers, e-

KEW

mail addresses, credit card information, law enforcement records or other identifying numbers or Protected Health Information, any financial identifiers, and other information that may be exempt from disclosure to the public or other unauthorized persons under either RCW 42.56.360, 42.56 RCW, or other state and federal statutes.

SPECIAL TERMS AND CONDITIONS

4. TERM OF AGREEMENT

The term of this Agreement begins on the date of execution of this Agreement. This Agreement will expire on August 31, 2018 or when DAPS is transferred to the DRIVES system, whichever is later.

5. GRANT OF LICENSE

To the extent DOL is permitted by applicable law, and subject to the terms and conditions of this Agreement, DOL hereby grants Licensee with a limited non-transferable license to have access to and use selected DOL vehicle, and/or driver Data available through DOL's DAPS system.

6. DATA OWNERSHIP

Licensee agrees that the Data is a valuable and sensitive property right of Licensor and that Licensor has sole and exclusive ownership of the Data. Licensor shall have the exclusive right to sell, license, disclose, distribute, transfer, or otherwise make available the Data to others.

7. ACCESS TO DATA

Each individual who will be accessing Data on behalf of the Licensee through the DAPS system must set up an individual Secure Access Washington account. All account transactions will be monitored by DOL's system to identify the information accessed through each of Licensee's accounts. Licensee immediately must revoke the access of any Authorized User when such access is no longer required.

Licensee must actively monitor access and use of Data by Authorized Users to ensure Data is accessed or used only for official job responsibilities. Licensee must immediately revoke the access of any Authorized User who accesses or uses Data without a Permissible Use.

Authorized User accounts are not interchangeable and cannot be shared; only the identified established person for any account may use that account. All Authorized Users must have an individual account, which is authorized by the Licensee.

The use of computerized applications (such as "bots") to access, retrieve, or store Data is prohibited.

8. DATA SECURITY AND SAFEGUARDING

Data provided pursuant to this Agreement includes public and Personal Information. Licensee acknowledges and agrees that it has a continuing obligation to comply with all federal and state laws, regulations, and security standards as enacted or revised over time, regarding Data Security, electronic data interchange and restricted uses of such information.

kel

Licensee shall further protect and safeguard all Personal Information against any and all unauthorized disclosure, use, or loss as set forth in Attachment A - *Data Security Requirements*.

At no time shall the Licensee or its employee or agent use, divulge, disclose, release, or communicate any Personal Information to any individuals or entities, or for any purposes, outside the scope of specific Permissible Uses allowed by this Agreement.

9. SECURITY BREACH

Licensee shall comply with all applicable laws that require the notification of individuals in the event of unauthorized release of Data or other event requiring notification. In the event of a breach of any of Licensee's security obligations, or other event requiring notification under applicable law, Licensee must perform the following:

- a) Notify DOL by telephone and e-mail of such an event within 24 hours of discovery:
DOL Help Desk, phone: (360) 902-0111,
DOL Help Desk, email: hlbhelp@dol.wa.gov
- b) Cooperate and facilitate with the notification of all necessary individuals. At DOL's discretion, Licensee may be required to directly perform notification requirements, or if DOL elects to perform the notifications, Licensee shall reimburse DOL for all costs associated with the notification.
- c) Licensee shall be responsible for any damages related to unauthorized use, disclosure, or security breach caused by Licensee.

10. PERMISSIBLE USE

Licensee may only use Data for purposes strictly limited to Licensee's functions as a governmental agency, and the purposes set forth in Licensee's application, as agreed upon and approved by DOL.

All other use of Data is strictly prohibited. DOL further retains the right to re-determine its approval for permitted uses and may cancel or restrict such uses at a later date if such uses do not comply with state law or DOL policy. If any purposes noted in the application are otherwise restricted by any terms of this Agreement, then the restrictions herein are controlling.

Licensee is strictly prohibited from using Data for purposes of investigating, locating, or apprehending individuals for immigration related violations.

Licensee shall also comply with all requirements set forth on Attachment B – *Permissible Use Requirements*.

11. INTERNAL CONTROLS

Licensee is responsible for ensuring that Authorized Users fully understand and abide by all terms and conditions of this Agreement; inherent in this requirement is that Licensee must institute proper training and disciplinary measures.

Licensee is strictly responsible for all actions of its Authorized Users in connection with the accessing of Personal Information under this Agreement.

If Licensee determines that an Authorized User has accessed or used Data for any purpose beyond what is authorized in this Agreement, it must notify DOL within ten (10) business days at: DataServices@dol.wa.gov. DOL may deny access to any Authorized User who violates any provision of this Agreement.

RCW

12. ANNUAL SELF-ASSESSMENT

Licensee shall self-assess its own entity to determine whether it is properly complying with the Data Security, Permissible Use and Internal Control requirements of this Agreement. At a minimum, the assessment must including the following:

- a) An evaluation to determine if Licensee is in compliance with the Data Security Requirements as set forth in Attachment A – *Data Security Requirements*;
- b) An evaluation to determine if Licensee is compliance with the Permissible Use Requirements set forth in Attachment B – *Permissible Use Requirements*;
- c) All Authorized User accesses have been revoked immediately when such access is no longer required;
- d) All Data Security Breaches and Permissible Use violations have been made to DOL in a timely manner; and
- e) All Data has been disposed of in a timely manner and as set forth in Attachment A – *Data Security Requirements*.

Upon request by DOL, Licensee must provide DOL with a written certification acknowledging the completion of an assessment.

If the assessment determines that Licensee is meeting all requirements outlined above, then Licensee's certification may simply note that the assessment was completed and no deficiencies were found. However, if deficiencies are discovered, Licensee must disclose all deficiencies by submitting a completed form, which will be provided by DOL. DOL and Licensee will then work together to determine the final actions needed in order to correct all deficiencies.

Failure to submit the certification upon DOL's request or failure to correct deficiencies may result in DOL terminating this Agreement.

The written certification must be executed by a manager, director, or officer of Licensee who has the expressed signatory authority to make such a certification on behalf of Licensee.

13. AUDITS

DOL has the right to request information and perform random audits on Licensee to verify its full compliance with the terms and conditions of this Agreement, and further to verify the accuracy of Licensee's self-assessed assessment. Inherent in this right, DOL may review any independent, third-party Data Security or Permissible Use audit performed on the Licensee within the last three years. Based on assessment findings, and on additional information gained by DOL, DOL may request that Licensee obtain further independent audits, and/or engage in specific corrective action to cure deficiencies.

If Licensee believes that any information given to DOL for these purposes is confidential or privileged information, Licensee may mark such information accordingly. Subject to the provisions of Chapter 42.56 RCW (Public Records Act), which applies to all state and local agencies, DOL will maintain the confidentiality of such information, and will provide Licensee with all notifications and protection rights afforded by the Public Records Act.

GENERAL TERMS AND CONDITIONS

14. ALTERATIONS AND AMENDMENTS

This Agreement may only be amended by mutual agreement of the Parties. Such

KEW

amendments are not binding unless they are in writing and signed by personnel authorized to bind each of the Parties.

Only DOL's Director or designated delegate by writing has the expressed authority to alter, amend, modify, or waive any clause or condition of this Agreement. Furthermore, any alteration, amendment, modification, or waiver of any clause or condition of this Agreement is not effective or binding unless made in writing and signed by DOL's Director or delegate.

15. COMPENSATION

This is a non-financial Contract and there are no costs to be charged to Licensee.

16. CONTRACT COMMUNICATIONS AND NOTICES

The Administrator is responsible for all general communications and notices pertaining to this Agreement on behalf of Licensee. Additional personnel may be identified for established specific purposes. If no additional people are named, then the Administrator will be the default reference person for all communications.

The use of email to the most current email address of the Administrator is an acceptable form of providing communication and notice for all purposes in this Agreement.

Licensee is responsible to notify the other in writing of any changes concerning the Administrator's name, phone number, or email address.

Licensee may contact DOL contract manager at DataServices@dol.wa.gov.

17. CONTRACT DISPUTE RESOLUTION

The Parties agree that time is of the essence when initiating the contract dispute resolution process. All disputes should be first resolved at the managerial level between the two entities.

18. GOVERNANCE

This Agreement is governed by the laws of the state of Washington and any applicable federal laws. Venue for any legal action arising from this Agreement is the Thurston County Superior Court.

In the event of an inconsistency in terms of this Agreement, or between the terms and any applicable statute or rule, the inconsistency will be resolved by giving precedence in the following order:

1. Applicable federal and Washington State laws, and regulations;
2. Specific Terms and conditions of this Agreement;
3. General Terms and conditions of this Agreement;
4. Attachments to this Agreement in sequential order; and
5. Any other documents and agreements incorporated herein.

19. INDEPENDENT CAPACITY

The scope of this Agreement maintains each Party's independent status as a self-governed entity, and nothing herein may be deemed as allowing any employee or agent of one Party to be considered as the employee or agent of the other Party.

KEL

20. INTEGRITY OF DATA

DOL compiles its Data based in part on the reporting of information from outside individuals and entities; as such, DOL may not be held liable for any errors which occur in compilation of Data. DOL may not be held liable for any delays in furnishing amended Data. DOL will make best efforts to ensure the DAPS system is available. However, DOL makes no guarantee of system availability, accuracy of data, or that the Data will meet the Licensee's needs. DOL may make changes to the DAPS system at any time to suit its business needs, without notification to Licensee.

21. INTERIM DISPOSAL OF DATA CONTAINING PERSONAL INFORMATION

Notwithstanding any permanent Data Disposal requirements set forth in Attachment A - *Data Security Requirements*, Licensee shall intermittently dispose of any Data containing Personal Information when Licensee's immediate use of that Data is no longer needed. Licensee is a government agency, and the Parties have mutually determined that the Licensee shall adhere to its required retention schedule.

22. RECORD MAINTENANCE

The Parties shall maintain all records relating to this Agreement, including all service and account records, including, but not limited to Appropriate Use Declarations and Permissible Use documentation, data security, and investigations related to use of Personal Information received from DAPS. All records and other material must be retained for six (6) years after expiration or termination of this Agreement.

If any litigation, claim, or audit is started before the expiration of the six-year period, the records shall be retained until all litigation, claims, or audit findings involving the records have been resolved including any appeals and remands.

23. RECORDS ACCESS AND INSPECTIONS

Licensee, at the request of DOL, must provide access to all records retained in connection with the receipt of Personal Information, as well as all other requirements under this Agreement. Upon request, such records must be made available for inspection, monitoring, review, audit and/or copying at no additional cost to DOL.

24. RECORDS REQUEST – PUBLIC RECORDS ACT

Both parties to this agreement are subject to the Chapter 42.56, RCW (Public Records Act). If Licensee believes that any information it gives to DOL is confidential or privileged in nature, then Licensee may mark such information accordingly. Subject to the provisions of the Public Records Act, DOL will maintain the confidentiality of such information, and will provide Licensee with all notifications and protection rights afforded by the Act.

If Licensee receives a public records request relating to any Personal Information accessed under this agreement, Licensee will maintain the full confidential nature of such information to the greatest extent allowed by law. Licensee will further provide notice to DOL consistent with the requirements of the Public Records Act, and will fully support DOL in maintaining the confidential nature of such information.

25. HOLD HARMLESS

Licensee shall hold DOL harmless for any damages or claims arising from its own acts and/or omissions, which includes those acts or omissions of its Authorized Users.

KEL

26. SEVERABILITY

If any provision of this Agreement or any provision of any document incorporated by reference shall be held invalid, such invalidity shall not affect the other provisions of this Agreement which can be given effect without the invalid provision, if such remainder conforms to the requirements of applicable law and the fundamental purpose of this Agreement, and to this end the provisions of this Agreement are declared to be severable.

27. TERMINATION

Termination of this Agreement may be terminated as set forth below. All termination matters may be applied as a suspension to the Access Period instead of a full termination, except that any suspension lasting longer than ninety (90) days will automatically terminate this Agreement.

A. Termination for Convenience

Either party may immediately terminate this Agreement at any time and for any reason upon providing written notice.

B. Administrative Terminations

If DOL's authority to actively engage in this Agreement is suspended or terminated, whether by lack of funding, or by any other governmental issue, including internal changes in policy, such a termination or suspension of authority will automatically cause a termination or suspension of this Agreement. DOL is to provide as much notice as possible when such termination or suspension appears eminent. This termination is without cause.

Included as an Administrative termination is that DOL will be cancelling the current DAPS system and instead will be moving DAPS to a new system known as DRIVES. The expected start date for DRIVES is September 4, 2018. When DOL switches to the DRIVES System, the current use of DAPS system will be terminated. Such termination of the current DAPS system will automatically cause the termination of this Agreement. Licensee will be allowed to establish a contract for the use of DAPS through the DRIVES system.

C. Termination for Cause

DOL's may terminate this Agreement, or any access privileges under this Agreement, for the violation of a material term or condition of this Agreement. DOL has sole discretion on whether such non-compliance is cause for immediate termination or suspension of the entire Agreement, whether it should suspend or terminate an Authorized User's access, or whether Licensee should be granted a cure process to correct any non-compliance without further actions.

28. WAIVER

The omission of either Party to exercise its rights under this Agreement does not preclude that Party from subsequent exercising of such rights and does not constitute a waiver of any rights.

KEU

Attachment A Data Security Requirements

1. DATA CLASSIFICATION

The classification of the Data shared under this Agreement includes:

- ☐ Category 1 – Public Information
- ☐ Category 2 – Sensitive Information
- ☒ Category 3 – Confidential Information (includes Personal Information)
- ☒ Category 4 – Confidential Information Requiring Special Handling (if Social Security Numbers are provided)

For all Confidential Data that is electronically stored, processed, or transmitted, Licensee shall apply the following requirements:

2. DATA SECURITY

Licensee must protect the confidentiality, integrity and availability of Data with administrative, technical and physical measures that meet generally recognized industry standards and best practices or standards established by the Office of the Chief Information Officer (OCIO).

Examples of industry standards and best practices include any of the following:

- a) ISO 27002
- b) PCI DSS
- c) NIST 800 series
- d) OCIO 141.10 (<https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets>)

NOTE: DOL has the right to implement security measures that may exceed OCIO or industry standards and best practices; if any security measures of this Agreement exceed OCIO or industry standards and best practices, then the higher DOL measures will apply. However, if any security measures of this Agreement fall below OCIO standards, then OCIO standards will apply.

3. NETWORK SECURITY

Licensee's network security must include the following:

- a) Network firewall provisioning
- b) Intrusion detection
- c) Quarterly vulnerability assessments
- d) Annual penetration tests.

4. ACCESS SECURITY

Licensee shall restrict Authorized User access to the Data by requiring a login using a unique user ID and complex password or other authentication mechanism which provides equal or greater security. Passwords must be changed on a periodic basis at least quarterly. The sharing of user ID and passwords is strictly prohibited. Licensee is solely responsible for protection of all of its user IDs and passwords, and is responsible for all breaches caused through the use of its user IDs and passwords.

5. APPLICATION SECURITY

Licensee shall maintain and support its software and subsequent upgrades, updates, patches, and bug fixes such that the software is, and remains secure from known

vulnerabilities. Licensee must secure web applications that minimally meet all the security controls as generally described in either:

- a) The Open Web Application Security Project Top Ten (OWASP Top 10), or
- b) The CWE/SANS TOP 25 Most Dangerous Software Errors

6. COMPUTER SECURITY

Licensee shall maintain computers that access Data by ensuring the operating system and software are updated and patched monthly, such that they remain secure from known vulnerabilities. Licensee computer device(s) must also be installed with an Anti-Malware solution and signatures updated no less than monthly.

7. DATA STORAGE

Licensee shall designate and be able to identify all computing equipment, on which Licensee stores, processes, and maintains Data. No Data at any time may be processed on or transferred to any portable storage medium. Laptop/tablet computing devices are not considered portable storage medium in this context provided that it is installed with end-point encryption.

8. ELECTRONIC DATA TRANSMISSION

Licensee shall maintain secure means (e.g., HTTPS or SFTP) for the electronic transmission or exchange of system and application data with DOL or any other authorized Licensee.

9. DATA ENCRYPTION

Licensee shall encrypt all Data, whether in transit or at rest, by using only NIST or ISO approved encryption algorithms; this includes all back-up copies of Data. Licensee further must install any laptop/notebook computing device, processing Data, with end-point encryption (i.e., full disk encryption).

10. DISTRIBUTION OF DATA

Licensee may only use and exchange Confidential Information for the purposes as expressly described and allowed in this Agreement. In addition to any other restrictions on Permissible Use, Confidential Information may not be distributed, repurposed or shared across other applications, environments, or business units of Licensee. Licensee must assure that no Confidential Information of any kind is transmitted, exchanged or otherwise passed to other contractors/vendors or interested parties except Licensee and/or Subrecipients who have an authorized legal Permissible Use according to this Agreement, and who are under contract with Licensee.

11. DATA DISPOSAL

Unless a more immediate disposal requirement is set forth in this Agreement, Licensee, upon termination of this Agreement, shall erase, destroy, and render unrecoverable all DOL Confidential Data and certify in writing that these actions have been completed within thirty (30) days of the termination of this Agreement. At a minimum, media sanitization is to be performed according to the standards enumerated by NIST SP 800-88r1 Guidelines for Media Sanitization.

12. OFFSHORING - ELECTRONIC

Licensee must maintain the primary, backup, disaster recovery and other sites for storage of Confidential Data only from locations in the United States.

KW

Licensee may not commit the following unless it has advance written approval from DOL:

- a) Directly or indirectly (including through Subrecipients) transmit any Confidential Data outside the United States; or
- b) Allow any Confidential Data to be accessed by Subrecipients from locations outside of the United States.

For all Confidential Data that is physically stored, processed, or distributed in a hardcopy format, Licensee shall apply the following requirements:

13. HARDCOPY STORAGE

To prevent unauthorized access to printed information obtained under this Agreement, and loss of, or unauthorized access to this information, printed copies must be stored in locked containers or storage areas, e.g. cabinets or vaults. Hard copy documents must never be unattended or in areas accessible to the public, especially after business hours.

14. HARDCOPY TRANSPORTATION

If hard copy documents containing Data are taken outside a secure area, those documents must be physically kept in possession of an authorized person, or a trusted courier providing tracking services. Records must be maintained for all transported hardcopies showing the person(s)/courier(s) responsible for such transportation, including the receiving party.

15. OFFSHORING - HARDCOPY

Licensee must maintain all hardcopies containing Confidential Information at locations in the United States.

Licensee may not directly or indirectly (including through Subrecipients) transport any Confidential Information outside the United States unless it has advance written approval from DOL.

HEW

Attachment B

Permissible Use Requirements

1. DATA USE

Licensee must institute and maintain written policies and procedures to ensure Data is only used as authorized herein. At a minimum, the policies and procedures will include training requirements for all personnel with access to Personal Information on the Permissible Use(s) of Data. Licensee must be capable of demonstrating the training and education was delivered to all applicable personnel who have are an Authorized User.

2. APPROPRIATE USE DECLARATION

Licensee must require all Authorized Users to sign an Appropriate Use Declaration. The Declaration must include a statement that the Authorized User understands and acknowledges:

1. His/her obligations and responsibility to use Personal Information only to accomplish his/her official job duties;
2. He/she will maintain the confidentiality and privacy of the information accessed;
3. He/she will not share Personal Information with unauthorized persons;
4. He/she will not use Data access for personal reasons or benefit; and
5. Misuse of any Personal Information may be considered a felony and may be punishable by fine or imprisonment.

Licensee must maintain the signed declaration. Licensee must provide copies of Appropriate Use Declaration upon request by DOL.

3. PERMISSIBLE USE EVALUATIONS

At least annually, Licensee must conduct a review of all Authorized Users' access and use of Confidential Information to ensure that such access and use is within official job duties.

4. SECURE USE

Licensee must maintain and support administrative, technical or physical methods used to monitor compliance with the Permissible Use(s) authorized in this Agreement across all Licensee business practices. Methods may include any of the following:

- a) View only access to Data
- b) System limitations or controls
- c) Confidentiality agreements

5. NON-CONFORMING PERMISSIBLE USE NOTIFICATION

Licensee shall notify DOL personnel in the event of confirmed unauthorized use of Data. Licensee must perform the following:

- a) Notify DOL by telephone and e-mail of such an event within 24 hours of discovery
DOL Contract Compliance Manager phone: (360) 902-3673,
DOL Data Sharing Unit email: DataServices@dol.wa.gov
- b) Identify the Data and non-conforming use of the Data.
- c) If the misuse is a criminal offense requiring notification to individuals, cooperate and facilitate with the notification of all affected individuals. At DOL's discretion, Licensee may be required to directly perform notification requirements, or if DOL elects to perform the notifications, Licensee may have to reimburse DOL for all costs associated with the notification.

**ATTACHMENT C
APPROPRIATE USE DECLARATION**

All DAPS Authorized Users must sign this form. Keep a signed copy of this declaration on file in your office—do not return it to the Department of Licensing.

DAPS users will:

1. Ensure the confidentiality and privacy of the information accessed.
2. Only use the information to accomplish official job duties.

DAPS users will not:

1. Use Data for purposes of investigating, locating, or apprehending individuals for immigration related violations.
2. Share the information with any unauthorized person.
3. Use the information for personal reasons or benefit.

Misuse of DAPS information is a felony and is punishable by fine and/or imprisonment.

I certify under penalty of perjury that I have reviewed the Data Licensing Agreement for DAPS, and understand the expectations and requirements therein.

X Rachel Ann Ealy-Williams Rachel E. Williams
TYPE or PRINT employee name Employee
signature Date

X Christopher G. Abela [Signature]
TYPE or PRINT supervisor name Supervisor
signature Date 5/31/2018